International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1372-1381 www.ijaem.net ISSN: 2395-5252

A Hybrid Framework ofCryptography andSteganography using Intelligent Agents

Emmanuel O. Ojei[1], Sylvanus O. Anigbogu[2], Kenechukwu S. Anigbogu[3]

[1,2,3]*Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria*

Submitted: 15-05-2021 Revised: 26-05-2021 Accepted: 28-05-2021

ABSTRACT: Information communication via email or the use of web browsers are not secure as sensitive information such as credit card information sent over such medium can be intercepted. There is a need for a private and secure communication for online users. To solve the issue, a combination of cryptography and steganography have been proposed to improve the security level of the system. This paper presents an agent-based tool that can help in selecting plain text to encrypt messages using cryptography and then recommend a suitable cover image to hide the encrypted message using steganography. The resulting stego-image can be transmitted without revealing the secret information that is being changed. The efficiency of the system is evaluated based on steganographic evaluation measures like PSNR and MSE. The result showed that the system satisfied the essentialssuch as capability, protection and robustness for secure data transmission.The outcome of the work is confirmed via performance analysis.

KEYWORDS: Cover-image, Stego-image, Stego-key, Cryptography, Encryption, Steganography, Steganalysis, Eavesdropper.

I. INTRODUCTION

Communication of secret information is a critical factor in the information era that we are now. Information technology continues to create challenges with increasing levels of sophistication evolving from stage to stage such as from documents, excel sheets, pdfs, pictures (JPEG and PNG), SMS, MMS, audio and video files. All these rich contents are communicated through email, YouTube and social media such as Twitter, WhatsApp, and Facebook, etc. People and organization rely on the Internet for the speedy delivery of information. Every year sharing of data or information around the world is getting doubled and in fact the World has gone data crazy [1]. On one side, through the Internet, roaming of data is rapidly growing each day. On the other side, communicating devices are growing in the ratio of many to one person. When communication takes place between parties that are located on the same secure network, these challenges can be considered as manageable. However, in the modern era, expectations are that one can travel the world and receive secret information at the same time without jeopardizing the confidentiality of secret information. In these situations, where the involved parties are spatially separate, the security of secret information cannot rely only on the advanced technologies of secure networks, because anadditional security mechanism should be incorporated. To communicate over an insecure channel, cryptography has been developed as a technique for constructing a secure logical channel over an insecure physical channel [2]. Cryptography is also referred to as information encryption while steganography is also called information hiding. These are the most significant techniques for information security [3].With cryptography, the secret information is altered in a way that it cannot be readable to eavesdroppers, but with steganography, the existence of the secret information is completely concealed from unauthorized persons.

The main goal of cryptography is to make the data to be kept secret into unintelligible format, in order to carry out confidential transmission over internet. Cryptography is based on the encryption algorithm, which encrypts the normal text to the unintelligible text, by employing a secret key.Cryptography fails, if the trespasser is able to approach the content of the cipher message. Encrypted data are even though unreadable, they give suspicion to the attackers. If they spend enough time, they can easily hack the original data. Alternative mechanisms that could improve upon these limitations should thus be investigated. Steganography is of one such mechanism that attempts to protect sensitive information from unauthorised parties.

Steganography is a technology that is used to hide secret information in digital media, thus hiding the fact that secret communication is taking place [4]. By hiding secret information in less suspicious digital media, well-known channels like e-mail and social networking sites are avoided, thereby reducing the risk of information being leaked in transit [5].Should an attacker attempt to intercept the communication through a man-in-the-middle attack, he would have no reason to suspect that he has intercepted anything more that an innocent image.

II. STATEMENT OF PROBLEM

Though Cryptography and Steganography try to protect data, both of these technologies alone are not perfect. Therefore, sometimes it is better to concatenate both approaches to improve the security level of the system. In such case, even if the communications existence was detected and the steganography was broken, the attacker still has to break the encryption to know the message. The statement of the problem for the work is to provide the security to the data while transferring over the internet. This can be achieved through developing an agent software that can help in making decision by choosing the suitable cover image to embed the specified secret imagefor steganography. This can improve data security and protect system from security violationsusingsteganography and cryptography techniquefor communication. This work is limited to the analysis of only digital images since they are the most popular and frequently used on the internet. It does not cover other carriers like text, audios, videos, protocols etc.

III. RELATED WORKS

Steganography and cryptography are two different techniques that maintain data confidentiality and integrity [6]. The purpose of steganography is to hide secret messages in digital media in a way that does not allow anyone to detect the existence of such secret messages[7].The main purpose of steganography is to communicate securely with secret messages through pictures [8]. Steganography does not change the structure of the secret message, but it hides inside the media so that the change is not visible [8]. While cryptography protects messages from unauthorized individuals by changing their meaning [9]. Steganography techniques depend on the confidentiality of the data encoding system [10] once the encoding system is known, the steganography system can be known or tracked. The stenographic technique enables the concealment of the fact that messages are being transmitted through digital media, such communication techniques are invisible between the sender and the receiver [11] while cryptography obscures the integrity of the information so that it is not understood by anyone but the sender and receiver [6]. Cryptography is a mathematical study that has links to aspects of information security such as data integrity, entity authenticity and data authenticity [12]. However, there is a need to provide further clarification of these techniques to assist in the understanding of the advantages of their combination.

The value of the confidential data obtained from a system is the most important thing to the attacker. The data may be compromised, distorted, or even deployed for future attacks by attacker [13]. A perfect way of solving these problems would be to exploit the advantage of cryptographic and steganographic techniques to develop a hybrid system which can be stronger than the individual strengths of the component techniques.

IV. SYSTEM ANALYSIS AND METHODOLOGY

Cryptographyis the methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. It is performed by converting messages or data into a different form, such that no-one can read them without having access to the 'key'. All encryption algorithms are based on two general principles: substitution, in which each element of the plaintext is mapped into another element, and transposition, in which elements of the plaintext are rearranged. The fundamental requirement is that no information be lost.

SecretKey(Symmetric): With secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called as symmetric encryption [9].

Public Key: In public key cryptography, encryption and decryption are performed using different keys. The sender need not send the decryption key. In this system a user can have public key and private key, the public key is known to all other users and private key known only for the user itself. So, encryption is performed using receiver’s public key so that the receiver can decrypt it with his private key [9].

AES algorithm for cryptography

Advanced Encryption Standard (AES) is a standard for the encryption of electronic data. The U.S. government held in 1997 and now use in worldwide. AES is a symmetric-key algorithm which means that the same key is used both of sender and receiver. This AES standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using key size of 128, 192, and 256 bits. The input, the output and the cipher key are used in Rijndael. It takes an input and output of certain block size of only 128 bits [9].

Steganography Techniques

Steganography is concealed writing and is the scientific approach of inserting the secret data within a cover media such that the unauthorized viewers do not get an idea of any information hidden in it. Steganography is an alternative to cryptography in which the secrete data is embedded into the carrier in such a way that only carrier is visible which is sent from transmitter to receiver without scrambling. Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. It does not replace cryptography but it can be used to improve the security of cryptography [10].

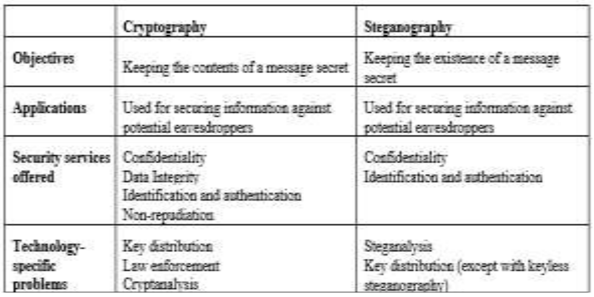
LSB –Steganography

In Least Significant Bit (LSB) steganography [11] embed the text message in least significant bits of digital picture. The data is embedded by replacing the LSB of cover carrier with the data to be sent.ie first read the cover image and text message which is to be hidden in the cover image, then convert text message in binary. Calculate LSB of each pixel of cover image. Replace LSB of cover image with each bit of secret message one by one so we get an image in which data is hidden.

Cryptography versus Steganography

To propose steganography as an alternative to cryptography, it requires a comparison between the two techniques. Table 2 presents a summary of the two techniques in terms of their security services, applications, problems, robustness and other criteria.

Table1. A comparative analysis of Encryption and Steganography [7]



	Cryptography	Steganography
Objectives	Keeping the contents of a message secret	Keeping the existence of a message secret
Applications	Used for securing information against potential eavesdroppers	Used for securing information against potential eavesdroppers
Security services offered	Confidentiality Data Integrity Identification and authentication Non-repudiation	Confidentiality Identification and authentication
Technology-specific problems	Key distribution Law enforcement Cryptanalysis	Steganalysis Key distribution (except with keyless steganography)

From Table 1, we observe that cryptography and steganography have two security services in common, namely confidentiality and identification. However, cryptography can offer two additional security services that are not offered by steganography at the moment, namely data integrity and non-repudiation. This work will adopt Object Oriented Analysis and Design (OOAD) to develop the new system using intelligent agents.

4.1 COMBINING CRYPTOGRAPHY AND STEGANOGRAPHY

Cryptography andsteganography have individually been insufficient for complete information security; therefore, a more reliable and strong mechanism can be achieved by combining both techniques. Combining these strategies can ensure an improved secret information security and will meet the requirements for security and robustness for transmitting important information over open channels.

A pictorial representation of the combined concept of cryptography and steganography is depicted in Figure 1

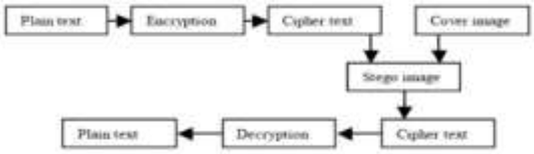


Figure 1: Combination of cryptography and steganography

Here, the information or data from the sender is taken as the plain text. Then, the plain text is converted into cipher text using any encryption method. The transformed cipher text can be used as the input for steganography. The key of cryptography is kept secret. Then the cipher text is embedded into the cover medium using steganography techniques. The cover image is transmitted to the receiver

Factors Affecting Combination of Cryptography and Steganography

Some factors that determine how efficient and powerful a technique include:

a. Robustness: Robustness refers to the ability of embedded data to remain unbroken if the stego image undergoes transformations, such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations.

b.Imperceptibility: The invisibility of a Steganographic algorithm is the first and foremost requirement, since the strength of Steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised.

c. Payload Capacity: It refers to the amount of secret information that can be hidden in the cover source. Steganography aims at hidden communication and therefore requires sufficient embedding capacity.

d. PSNR (Peak Signal to Noise Ratio): It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the reliability of its representation. This ratio is mainly used as a quality measurement between the original and compressed image. The higher the PSNR, the better the quality of the compressed image

e. MSE (Mean Square Error): Mean Squared Error is the average squared difference between a reference image and a distorted image. An Image Steganography technique is able if it gives low MSE.

Application of Steganography

a. Secret Communication: By using Steganography, two parties can communicate secretly without anyone knowing about the communication. In Cryptography, the message is encoded but its presence is not hidden. Thereby, drawing unwanted attention. On the other hand, Steganography hides the existence of message in some cover media.

b. Copyright Protection: The secret message is embedded in the images which serves as the watermark and thus identify it as an intellectual property which belongs to a particular owner. This is basically related to watermarking.

c. Feature Tagging: Features such as captions, annotations, name of the individuals in a photo or location in a map can be embedded inside an image. Copying the stego image also copies all of the embedded features and only parties who possess the decoding stego key will be able to extract and view the features.

d. Use by terrorists: Steganography can also be used by terrorists in order to hide their secret messages in innocent, cover sources to spread terrorism across the country.

e. Digital Watermarking: This is the most important applications of Steganography. It basically embeds a digital watermark inside an image. This Watermark is used to verify the authenticity or integrity of the carrier signal. It is highly used for tracing copyright infringements and for banknote authentication

4.2 INTELLIGENT AGENTS

Outside the realm of computers, the term agent is well defined. It derives from the concept of agency, which is to employ someone (like a theatrical agent) to act on your behalf. An agent represents a person or organization and interacts with others to accomplish a predefined task. In the computer realm, agent also called software agent is a software that assists people and acts on their behalf. Intelligent agents work by allowing people to delegate work that they could have done to the agent software. Agents, just as assistants can, automate repetitive tasks, remember things you forgot, intelligently summarize complex data, learn from you, and even make recommendations to you." [14]. A good working definition of an agent is that:is anything that can be viewed as perceiving its environment through sensors and acting on that environment through effectors." [15].

Functions of an Intelligent Agent

An intelligent agent continuously performs three functions:

a.Perception of dynamic conditions in the environment,

b. Action to affect conditions in the environment,

c. Reasoning to interpret perceptions, solve problems, draw inferences, and determine actions

Common Attributes of Intelligent Agents

The common attributes of intelligent agents:

•Autonomy: being autonomous, meanthat agentsare independent and capable of working without

human supervision.This is one attribute that distinguish agent from objects.
•Self-learning: Agent are capable of changing their behaviour according to their accumulated knowledge.
•Proactive: Agent are capable of making decisions based on its own initiative.
•Communication: Agent are able to communicate with other systems and agents, while also communicating with the end user in natural language.
•Co-operation: some of the more advanced agents act in unison with other agents to carry out complex tasks.
•Mobility: Agent are mobile,enabling it to travel throughout computer systems in order to accumulate knowledge and carry out tasks.
•Goal Driven: Agentshave goals, a user-defined purpose, and then act in accordance with that purpose.

V. SYSTEM DESIGN

In this work, the agent system is the process in which cryptography and steganography are used. The design for combining two different techniques is purely performed in the Java programming language using the Least Significant Bit (LSB) steganography technique and block cryptography AES (128 bits). The system architecture will be based on the Jade framework that works as a development platform, receiving the requests, processing their respective requisitions and making informed decisions. Figure 2 depicts the architecture of the new system.

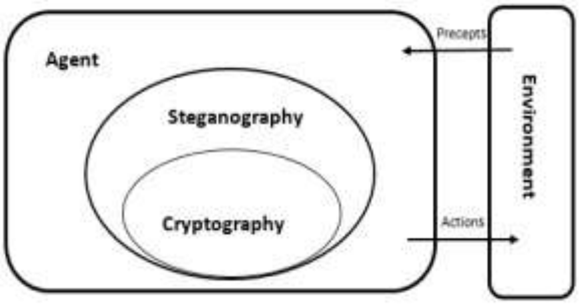


Figure 2: The architecture of the system

The newsystem design consists of four modules which include:

- Encryption Module
- Steganography Module
- Extraction Module
- Decryption Module

The detailed description of the four modules is depicted in Figure 4. Cryptography Module transforms the secret message into cipher text and then, Steganography Module is used to embed the cipher text inside the image using the LSB substitution method. Modules Cryptography and Steganography work on Sender side. When the embedded image is sent over the communication channel, the receiver side Modules Extraction and Decryption will start to act. Extraction first extracts the hidden message from the image. Now, the message is a transformed version of the original one. Then, Decryption will convert the message into its original form using the Cryptography algorithm. Finally, the secret message will be revealed.

Encryption Module

The encryption module represents all the actions taken to encrypt the secret message. The block cryptography AES (128 bits) is used. Here, the system reads the secret message to find the length of the message going to be securely communicated. It will take the first letter in the message, convert into ASCII value. Mod each digit of ASCII value by length and if the mod value is zero, it will left shift the binary value of the ASCII equivalent to their position value, then start to place the transformed letter from the first position onwards. Fill the remaining position by the untransformed letters. If the mod value is not zero, then leave the letter in their position itself. The system will take the next letter, repeat from step 4 to 7 up to the length of the message until the original message is transformed into a new one.

Steganography Module

The steganography module represents all the actions taken to hide the above generated transformed secret message. The Least Significant Bit (LSB) steganography method is used. The system will load the cover image and will read the secret message which is to be hidden in the cover image, which then convert secret message in binary. The system will select the pixel position for embedding and the positions for hiding the message inside the cover image are randomly selected. It will calculate LSB of each pixel of cover image, the first three LSBs are reserved for embedding hidden pixel position, starting position of hiding and the length of the message. Replace LSB of cover image with each bit of secret message one by one so that we get an image in which data is hidden, called stego image.

Extraction Module

The extraction module represents all the actions taken to retrieve the transformed secret message from the stego image. The system will read the stego image which is the result of steganography module. Extract the key information. The position of the hidden pixels and starting position of hidden and length of the message is given in the first three LSBs, then, extracting that first three LSBs, key information for extraction is filtered. Retrieve the embedded secret bits on the key information. Then concatenate all bits together and convert into ASCII value.

Decryption Module

The decryption module represents all the actions taken to retrieve the cipher text. The system reads the cipher text and the ASCII values of cipher text is now converted into original alphabets. The encryption algorithms will be applied in the reverse order which will retrieve the original alphabets that is nothing but the secret message.

Figure 3 presents a flowchart that shows the detailed description of the four modules.

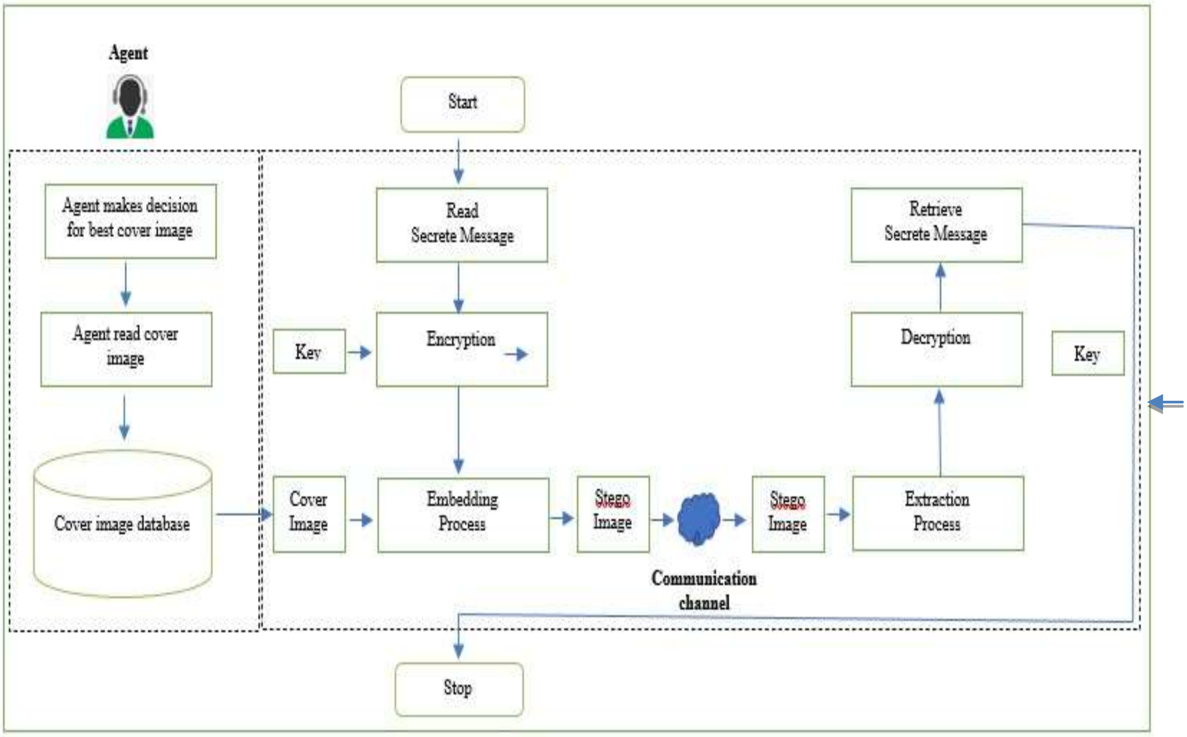


Figure 3: System Flowchart

VI. RESULTS AND DISCUSSION

This section represents the result of using the proposed method to hide secret information.

Here, the agent helps to choose appropriate cover image which is selected from the database. The cover image and stego image is shown in figure 4, 5, and 6 (a & b) with their histograms. The stego image is looking similar to the cover image, but with the use of the histogram and visually looks like a small change due to the changes in the least pixel value of the image. In the encryption process and decryption process, the quality of an image should be degraded to preserve the quality of the image.

To evaluate the performance of the proposed system, the Peak Signal to Noise Ratio (PSNR) and MSE are calculated. PSNR is the accurate metrics used to judge the imperceptibility of stego images. PSNR is used as a quality measurement between the cover (captured image) and stego (embedded image) images. Here, both cover (X) and stego (Y) images are colorful and JPEG images. The quality of the image is acceptable, if the PSNR value is higher than 40dB.

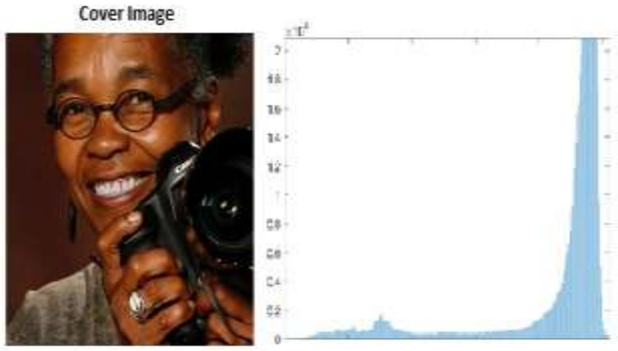


Figure 4a: Cover Image and Histogram

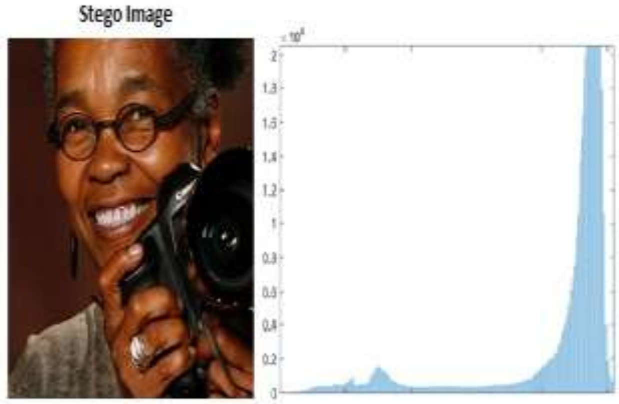


Figure 4b: Stego Image and Histogram

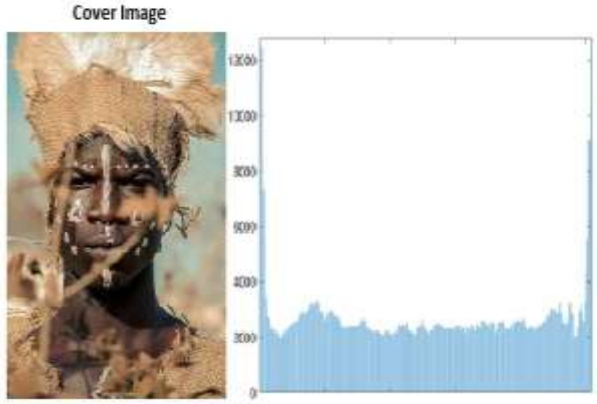


Figure 5a: Cover Image and Histogram

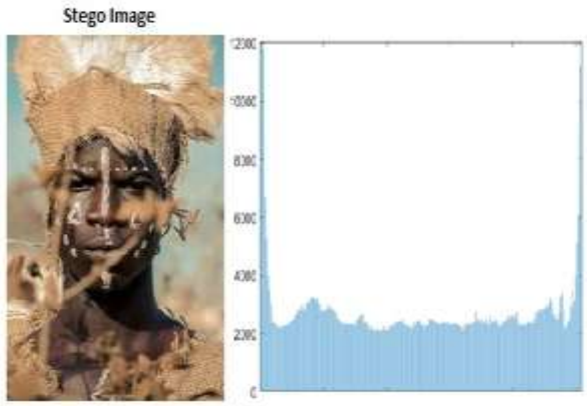


Figure 5b: Stego Image and Histogram

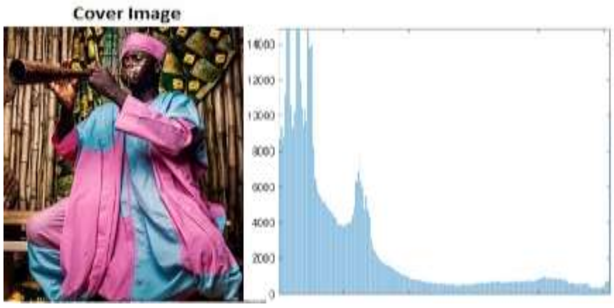


Figure 6a: Cover Image and Histogram

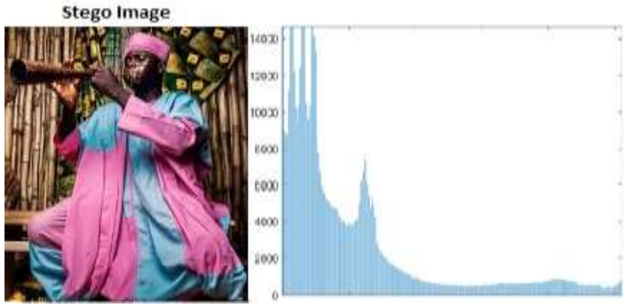


Figure 6b: Stego Image and Histogram

To measure PSNR for color images, the formula given in Equation (2) is used.

PSNR = 10 * log(2552 /MSE) (2)

To evaluate the Peak Signal to Noise Ratio, then we need to find the Mean Square Root Error (MSE) values. MSE values are calculated using Equations (3).

$$MSE = \frac{\sum_{M,N}[CI(m,n)-SI(m,n)]^2}{M*N} \qquad (3)$$

and P= max(max(X), max(Y))

P is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255. Here, R is 255

Where M and N are the number of rows and columns in the input images such as cover image (X) and stego image (Y).

The PSNR represents a meter of the elevation error. The higher the PSNR, the more reliable the quality of the stego image.

The histogram shows the frequency distribution of a set of continuous data used to inspect the underlying distribution. It also shows the changes made during the embedding process.

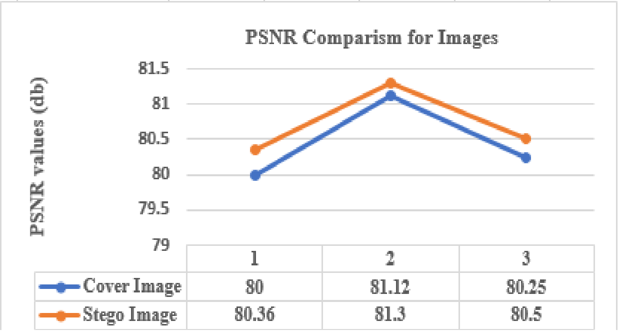


Figure 7: PSNR comparison for Cover and Stego Images

Table 2: Parameter values for the proposed system

Features	**Proposed**
PSNR	High
MSE	Low
Security	High
Robustness	High
Imperceptibility	High

The results of the new system against the various parameters show high PSNR values, low MSE values, high security, high robustness and high imperceptibility. This means the image has very good quality and similar at the size and quality to the stego image.

CONCLUSION

This work has presented an agent-based system for combining cryptography and steganography using the LSB steganography technique and block cryptography AES (128 bits) for digitalimages. The results have proven that the new hybrid methodology offered good concealment and a highly secured method for communication with the agent helping to identify best components which offered benefits. The goal of steganography, especially combined with cryptography, is a powerful instrument which enabled people to communicate without possible eavesdroppers and even knowing, there is a form of communication in the first position with good image quality. The primary advantage of this system is that the method applied for encryption is very strong and difficult to notice. Future work can be done to apply new techniques for secrete communication that provide better security.

REFERENCES

[1]. Jeff Desjardins 2015, visualcapitalist. [online]. [Accessed 3September 2017]. Available from World Wide Web:<http://www.visualcapitalist.com/evolution-of-data/>

[2]. Gollmann, Dieter"Computer Security." (1999-02-16).Wiley Interdisciplinary Reviews: Computational Statistics 2, 544-554

[3]. Moody G D, Siponen M and Pahnila S 2018 Toward a unified model of information security policy compliance MIS Quarterly 42 1.

[4]. Jamil, Tariq. "Steganography: The art of hiding information in plain sight." Journal of IEEE Potentials (1999): 10-12.

[5]. Artz, Donovan. "Digital steganography: hiding data within data." IEEE Internet computing 5.3 (2001): 75-80

[6]. Joseph A and Sundaram V 2011 Cryptography and steganography–A survey.

[7]. Laskar S A and Hemachandran K 2012 Combining JPEG steganography and substitution encryption for secure data communication Computer Science\& Information Technology (CS\& IT).

[8]. Johnson N F and Jajodia S 1998 Exploring steganography: Seeing the unseen Computer 31.

[9]. Katz J, Menezes A J, Van Oorschot P C and Vanstone S A 1996 Handbook of applied cryptography CRC press.

[10]. Conway M 2003 Code wars: steganography, signals intelligence, and

terrorism Knowledge, Technology & Policy 16 45-62.

[11]. Walia E, Jain P and Navdeep N 2010 “An analysis of LSB & DCT based steganography”. GlobalJournal of Computer Science and Technology.

[12]. Zaidan B B, Zaidan A A, Al-Frajat A K and Jalab H A 2010 On the differences between hiding information and cryptography techniques: An overview Journal of Applied Sciences(Faisalabad) 10 1650-1655.

[13]. Seth D, Ramanathan L and Pandey A 2010 Security enhancement: Combining cryptography and steganography International Journal of Computer Applications 3-6

[14]. Gilbert, D. “Intelligent Agents: The Right Information at the Right Time.” IBM white paper, citeseer.nj.nec.com/context/1105800/0,May 1997.

[15]. Russell, J., and P. Norvig. Artificial Intelligence: A Modern Approach. Upper Saddle River, NJ: Prentice Hall, 1995.

[16]. Almuhammadi S and Al-Shaaby A 2017 A survey on recent approaches combining cryptographyand steganography Computer Science Information Technology (CS IT).

[17]. Mitali V K and Sharma A 2014 A survey on various cryptography techniques International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 3 307-312.

[18]. Jirwan N, Singh A and Vijay D S 2013 Review and analysis of cryptographytechniques International Journal of Scientific & Engineering Research 4 1-6.